

Citigroup Inc.  
1101 Pennsylvania Avenue NW  
Suite 1000  
Washington, DC 20004  
202/879-6877  
Fax 202/879-6831

August 2, 2005

Via Overnight Mail, Electronic Delivery and Facsimile

The Honorable John C. Watkins, Chairman  
Privacy Advisory Committee  
Joint Commission on Technology and Science (JCOTS)  
General Assembly Building  
901 Capitol Street, Second Floor  
Richmond, VA 23219

**Re: Privacy Advisory Committee - Data Security**

Dear Senator Watkins:

On behalf of Citigroup, thank you for the opportunity to submit some thoughts and comments on the data security breach issue being considered by the Privacy Advisory Committee of the Joint Commission on Science and Technology (JCOTS).

Citigroup is the world's leading integrated financial services company. Our business lines include Citibank, CitiFinancial, and Primerica Financial Services. Our presence in the Commonwealth is very significant, with over 80 business locations and hundreds of employees providing credit services and a variety of financial products to Virginians. Because we provide these financial services, we are required by law to maintain certain data relating to our customers. Through the proper use of this information, we are able to assess credit risk, maintain accounts, and offer services and products that best fit a specific customer's needs. Furthermore, in recognizing our obligation to the consumers we serve, Citigroup has initiated several industry-leading programs, including *Citi Identity Theft Solutions*, our Fraud Early Warning Program, and an Internet Security Specialists team to assist customers in the event of identity theft or fraud.

As you know, over the past several years consumers, policymakers, and the financial services community have become increasingly focused on the myriad issues surrounding the retention and security of consumer data. In 2002, California became the first state to enact a law on data breach and security. In March 2005, several federal agencies published the *Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and customer Notice*. Also, over 25 states, including Virginia, considered legislation in this policy area during their 2005 legislative sessions.

Perhaps most significantly, on July 28th, the Commerce Committee of the United States Senate became the first congressional committee to consider, and unanimously approve, a broad identity theft protection bill. The bipartisan measure, S. 1408, would, among other things, require nonfinancial companies, such as data brokers that handle sensitive personal information, to maintain the security and confidentiality of the information by implementing certain safeguards specified by the Federal Trade Commission. The bill would also allow consumers - - regardless of whether they are the victims of a security breach - - to put a "freeze" on their credit reports. The United States House of Representatives is also demonstrating profound interest in this issue.

Page 2  
August 2, 2005

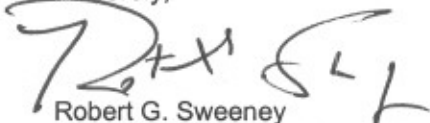
A subcommittee of the House Energy and Commerce Committee held a hearing on July 28th titled: "Data Security: The Discussion Draft of Data Protection Legislation." Many congressional observers anticipate further hearings and debate in September.

With respect to database security legislation at the state level, many legislatures have wisely included triggers for companies to use in determining when notification is necessary. Additionally, some states have enacted, and Citigroup supports, legislation clarifying that any financial institution that is subject to and in compliance with the security breach guidelines or regulations of its primary functional regulator is thereby deemed to be in compliance with state law. Delaware HB 116, recently signed by Governor Minner (*attached for your consideration*), provides: "Under this chapter, an individual or a commercial entity that is regulated by State or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional State or federal regulator is deemed to be in compliance with this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with the maintained procedures when a breach occurs."

As a national corporation with customers in all 50 states, Citigroup supports a uniform standard for resolving the relevant policy issues and questions posed by any state legislation, such as Virginia HB 2721, that might mandate consumer notification in the event of a database breach. As noted above, both federal regulators and Congress are taking decisive action in this area, and additional steps are likely. We respectfully request that the JCOTS Privacy Advisory Committee consider both the unique responsibilities of national financial services providers, and the ongoing federal activity in this area, as it conducts its study. We think that a cautious approach which is consistent with the efforts of federal regulators and Congress would be appropriate and responsive to the very legitimate concerns that have been raised by all who are interested in these issues.

Thank you again for the opportunity to provide comments on this important matter. I look forward to working with you, and all members of JCOTS, as this issue moves forward.

Sincerely,

A handwritten signature in black ink, appearing to read "R. G. Sweeney", is written over the typed name.

Robert G. Sweeney  
Vice President, Mid-Atlantic Region  
State & Local Government Relations

Attachment

cc: Lisa Wallmeyer, Executive Director of the Joint Commission on Technology and Science  
Alexander Macaulay, Macaulay & Burtch, PC

SPONSOR: Rep. Gilligan & Rep. Stone, & Sen. Sokola  
Reps. Booth, Buckworth, Ennis, Ewing, Fallon, George,  
Hall-Long, Hocker, Johnson, Keeley, Longhurst,  
McWilliams, Mulrooney, Plant, Roy, Schooley,  
Schwartzkopf, Ulbrich, VanSant, Viola, Williams; Sens.  
Bunting, Cook, Henry

HOUSE OF REPRESENTATIVES

143rd GENERAL ASSEMBLY

HOUSE BILL NO. 116  
AS AMENDED BY  
HOUSE AMENDMENT NO. 1 AS AMENDED  
BY  
HOUSE AMENDMENT NO. 1 TO HOUSE  
AMENDMENT NO. 1 HOUSE AMENDMENT  
NO. 2 TO HOUSE AMENDMENT NO. 1 HOUSE  
AMENDMENT NO. 3 TO HOUSE AMENDMENT  
NO. 1 HOUSE AMENDMENT NO. 4 TO HOUSE  
AMENDMENT NO. 1 & HOUSE AMENDMENT  
NO. 6 TO HOUSE AMENDMENT NO. 1

AN ACT TO AMEND TITLE 6 OF THE DELAWARE CODE RELATING TO COMPUTER SECURITY BREACHES.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

“Section 1. Amend Title 6 of the Delaware Code by adding thereto a new chapter to read:

‘CHAPTER 12B. COMPUTER SECURITY BREACHES

§12B-101. Definitions.

For purposes of this chapter:

(1) ‘breach of the security of the system’ means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;

(2) ‘commercial entity’ includes corporations, business trusts, estates, trusts, partnerships,

limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit;

(3) 'personal information' means a Delaware resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

- (i) Social Security number;
- (ii) driver's license number or Delaware Identification Card number; or
- (iii) account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

The term 'personal information' does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records;

(4) 'notice' means:

- (i) written notice;
- (ii) telephonic notice;
- (iii) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in §7001 of Title 15 of the United States Code; or
- (iv) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$75,000, or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:
  - a. e-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Delaware residents; and
  - b. conspicuous posting of the notice on the Web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and
  - c. notice to major statewide media.

§12B-102. Disclosure of breach of security of computerized personal information by an individual or a commercial entity.

(a) An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or

the commercial entity shall give notice as soon as possible to the affected Delaware resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

(c) Notice required by this chapter may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this chapter must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

§12B-103. Procedures deemed in compliance with security breach requirements.

(a) Under this chapter, an individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with its policies in the event of a breach of security of the system.

(b) Under this chapter, an individual or a commercial entity that is regulated by State or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional State or federal regulator is deemed to be in compliance with this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with the maintained procedures when a breach occurs.

§12B-104. Violations.

Pursuant to the enforcement duties and powers of the Consumer Protection Division of the Department of Justice under 29 Del. C. §2517, the Attorney General may bring an action in law or equity to address violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do not relieve an individual or a commercial entity subject to this chapter from compliance with all other applicable provisions of law.”.